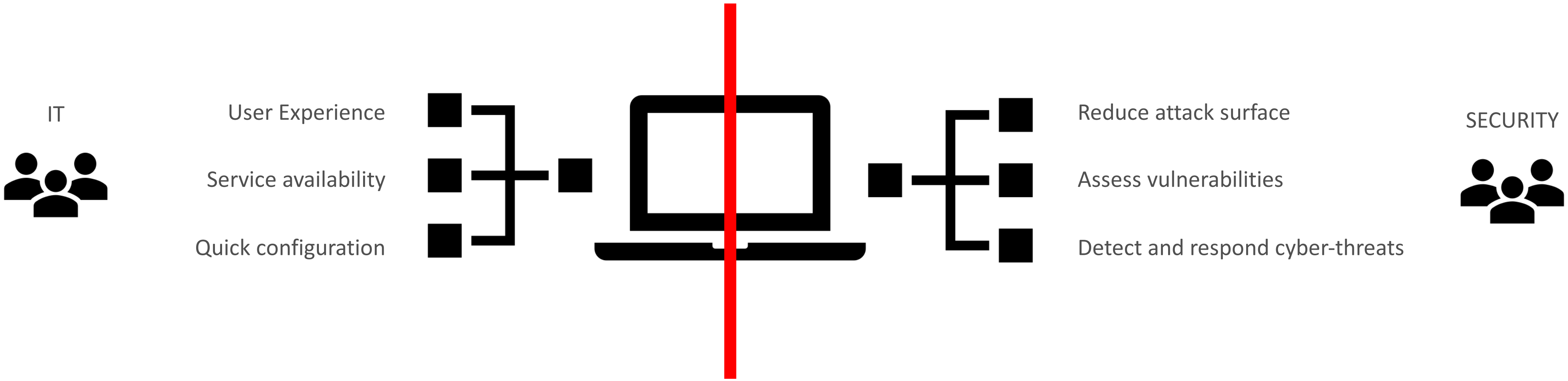
WHAT'S BEHIND MICROSOFT DEFENDER ADVANCED THREAT PROTECTION

COME JOIN THIS SESSION WHERE A MEMBER OF THE PRODUCT ENGINEERING TEAM WILL WALK YOU THROUGH A MODERN ENDPOINT SECURITY STACK WITH PRACTICAL EXAMPLES ON REAL CYBER-ATTACKS.

HOSTED BY

MILAD ASLANER

@MiladMSFT



IT

User Experience

Service availability

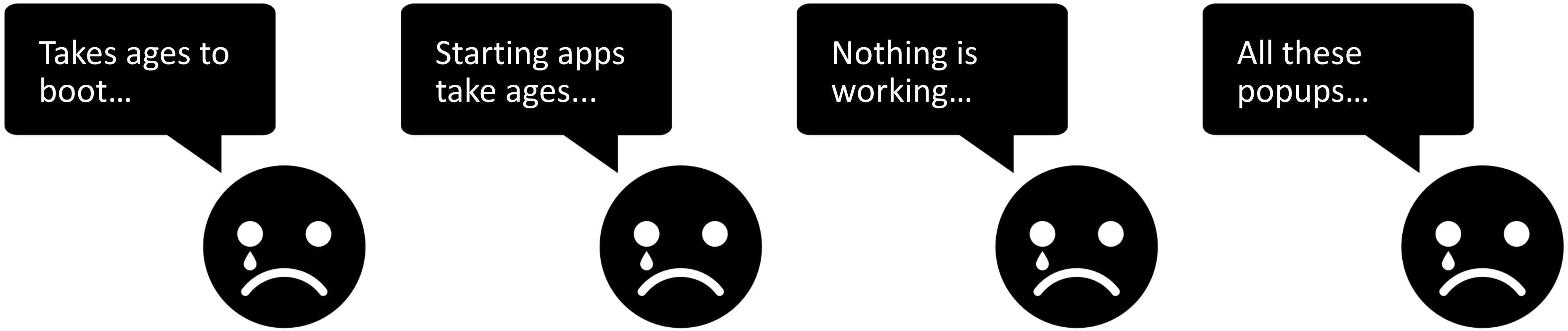
Quick configuration

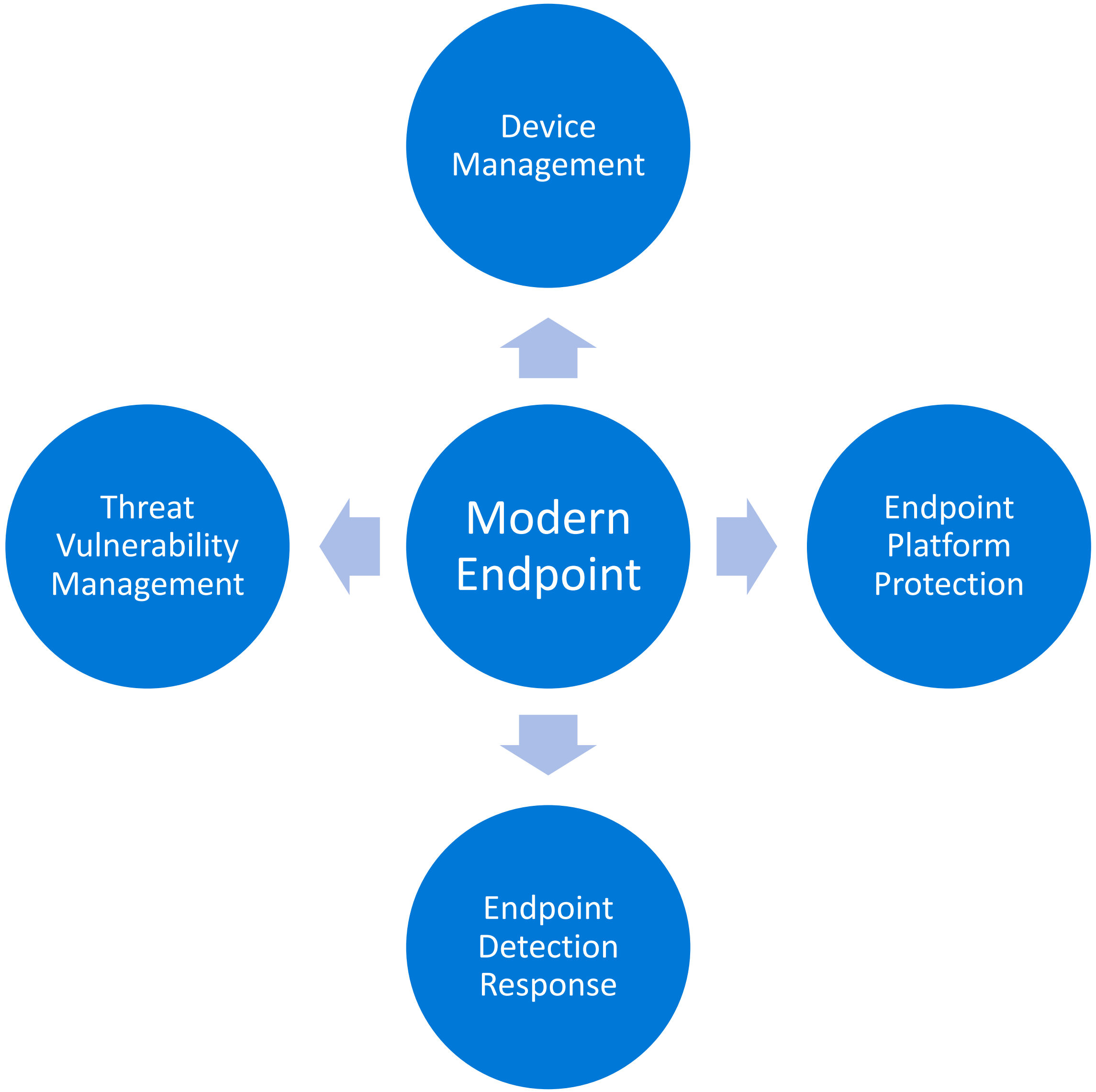
Reduce attack surface

Assess vulnerabilities

Detect and respond cyber-threats

SECURITY





Device Management

Threat Vulnerability Management

Modern Endpoint

Endpoint Platform Protection

Endpoint Detection Response

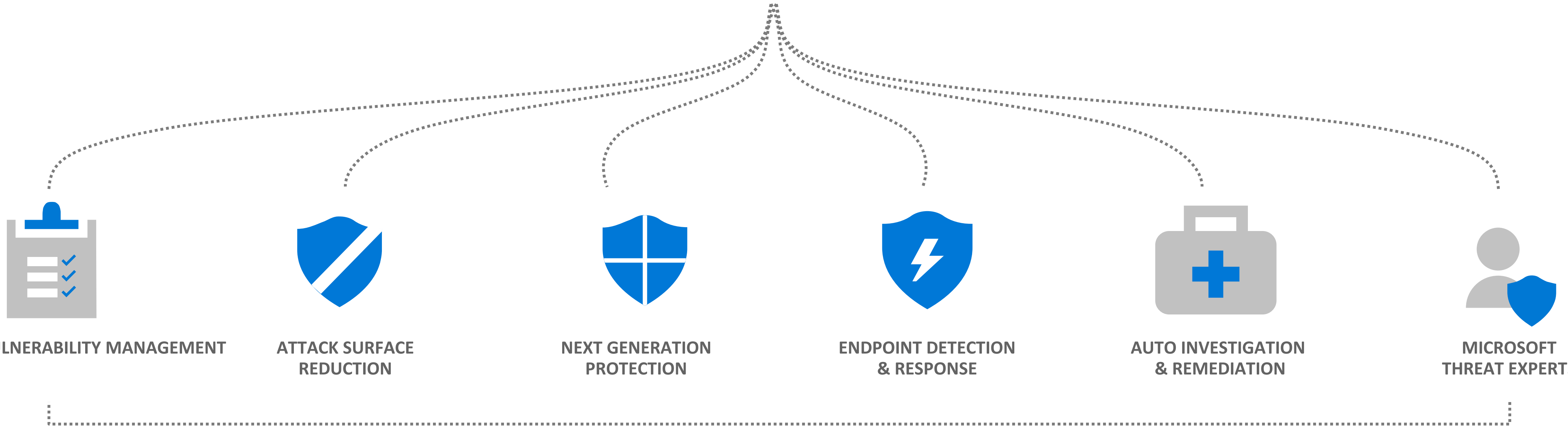
Microsoft Defender Advanced Threat Protection (ATP)

❤

Microsoft Intune

Microsoft Defender
Advanced Threat Protection

Built-in. Cloud-powered.



THREAT & VULNERABILITY MANAGEMENT

ATTACK SURFACE REDUCTION

NEXT GENERATION PROTECTION

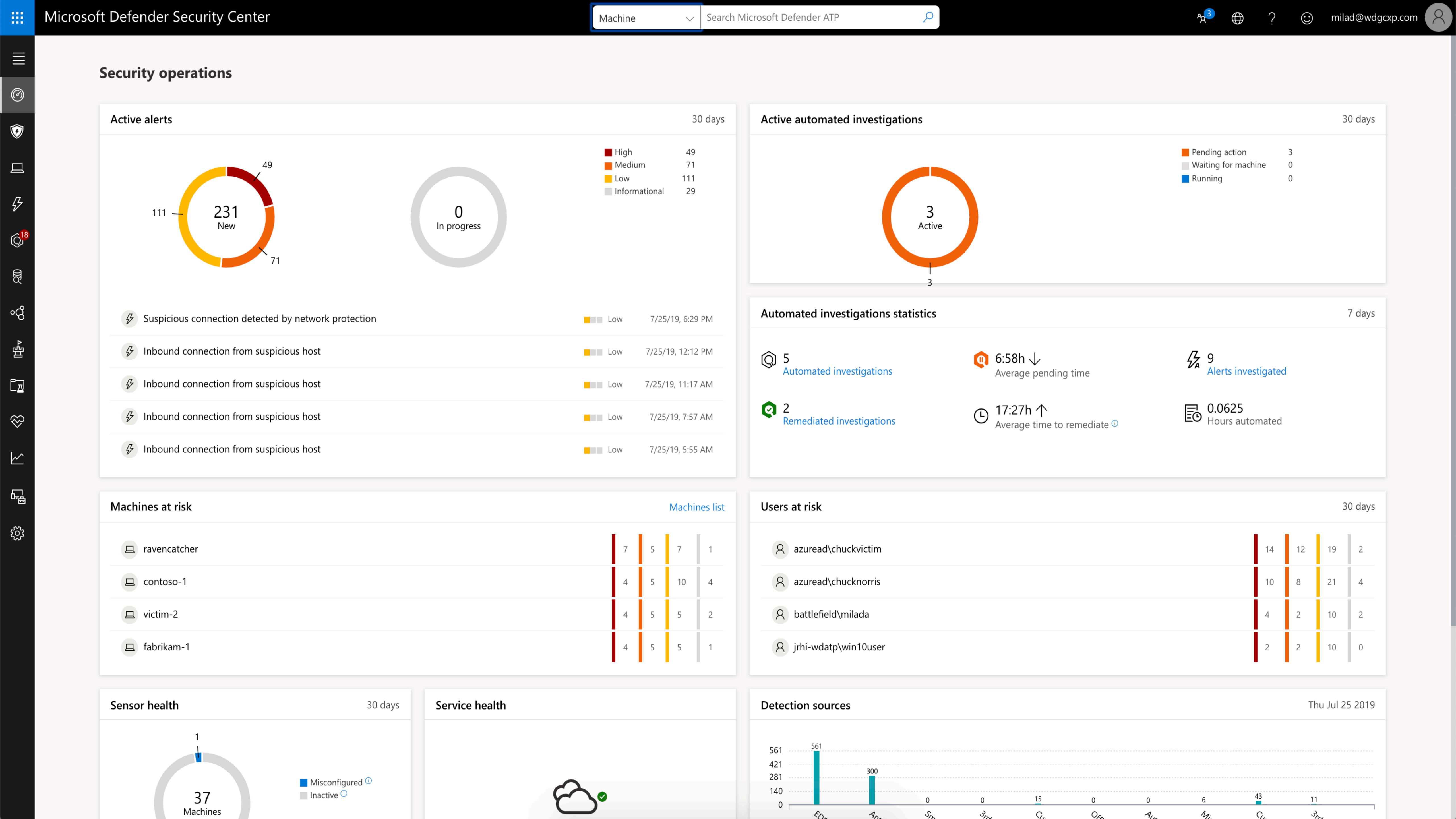
ENDPOINT DETECTION & RESPONSE

AUTO INVESTIGATION & REMEDIATION

MICROSOFT THREAT EXPERTS

CENTRALIZED CONFIGURATION AND ADMINISTRATION, APIS

DEMO TIME



Microsoft Defender Security Center

Machine

Search Microsoft Defender ATP

milad@wdgcxp.com

Security operations

Active alerts

30 days

231 New

0 In progress

🟥 High	49
🟧 Medium	71
🟨 Low	111
⬜ Informational	29

Suspicious connection detected by network protection	Low	7/25/19, 6:29 PM
Inbound connection from suspicious host	Low	7/25/19, 12:12 PM
Inbound connection from suspicious host	Low	7/25/19, 11:17 AM
Inbound connection from suspicious host	Low	7/25/19, 7:57 AM
Inbound connection from suspicious host	Low	7/25/19, 5:55 AM

Active automated investigations

30 days

3 Active

🟧 Pending action	3
⬜ Waiting for machine	0
🟦 Running	0

Automated investigations statistics

7 days

5 Automated investigations

6:58h ↓ Average pending time

9 Alerts investigated

2 Remediated investigations

17:27h ↑ Average time to remediate

0.0625 Hours automated

Machines at risk

Machines list

ravencatcher	7	5	7	1
contoso-1	4	5	10	4
victim-2	4	5	5	2
fabrikam-1	4	5	5	1

Users at risk

30 days

azuread\chuckvictim	14	12	19	2
azuread\chucknorris	10	8	21	4
battlefield\milada	4	2	10	2
jrhi-wdatp\win10user	2	2	10	0

Sensor health

30 days

37 Machines

🟦 Misconfigured ⓘ

⬜ Inactive ⓘ

Service health

Detection sources

Thu Jul 25 2019